IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Liqun Chen	)	Examiner: Simitoski, M.J.
		)	
Serial No.	10/613,750	)	Art Unit: 2134
		)	
Filed:	7/3/2003	)	Our Ref: B-5154 621086-5
		)	300201957-3
For:	"Method and Apparatus for Generating a Cryptographic Key"	)	Date: March 19, 2008
		)	Re: *Petition for*
		)	*Reconsideration Under*
		)	*37 CFR 1.181*
		)	

PETITION FOR RECONSIDERATION UNDER 37 CFR 1.181

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Notice from the Office of Petitions dated March 4, 2008, wherein a petition for withdrawal of abandonment for the above-identified application (filed on January 22, 2008) is dismissed, Applicants submit a petition for reconsideration under 37 CFR 1.181.

Please charge to deposit account no. 08-2025 any additional fee required or credit for any excess paid.

STATEMENT OF THE FACTS INVOLVED

1. On May 15, 2007 the USPTO issued a Non-Final Official Action setting forth a statutory time period for reply of three months from the mailing date of the Official Action, in the instant case, August 15, 2007.

2. The Applicant mailed by way of the United States Post Office a response to the official action on August 15, 2007. The response contained a certificate of mailing or transmission, in accordance with 37 CFR § 1.8(a)(1)(ii). The certificate was signed and stated the date of transmission. The response also contained a Postcard to be returned by the USPTO to the attorney of record. A complete copy of the response as filed is enclosed with the present petition as Exhibit 1.

3. The Postcard mailed with the response on August 15, 2007, containing the USPTO stamp of receipt dated August 20, 2007, was received by the office of the attorney of record on August 24, 2007. A copy of the Postcard with the USPTO stamp of receipt is enclosed with the present Petition as Exhibit 2.

4. On January 7, 2008, the USPTO sent erroneously a Notice of Abandonment to the Applicant, stating that the application had been abandoned in view of the Applicant's failure to timely file a proper reply within the statutory period of three months from the mailing date of the Official Action.

5. On January 22, 2008, the Applicant submitted a Petition for Withdrawal of Abandonment. The Applicant further submitted as an attachment to the Petition copies of the documents attached herein as Exhibit 1 and Exhibit 2.

SUBMISSIONS

As requested, the Applicant submits attached hereto a Statement by the attorney of record attesting on personal knowledge that the documents in question were mailed on August 15, 2007.

The Applicant submits that the present petition to withdraw the holding of abandonment is filed within the 2-month time limit set forth in 37 CFR § 1.181(f).

The Applicant submits that the petition should be granted under at least one of the following standards:

1) 37 CFR § 1.8(b) 'Certificate of Mailing' standard. In particular, the Applicant submits that the present petition and its enclosures satisfy to the requirements set forth in subparagraphs (1) to (3) of 37 CFR § 1.8(b).

2) MPEP 503 Postcard Receipt as Prima Facie Evidence that the USPTO indeed received Applicant's response.

ACTION REQUESTED

1. The USPTO is respectfully requested to deem the Response and certificate of mailing enclosed as Exhibit 1 as properly mailed on August 15, 2007 and as evidence of the mailing date of the response.

2. The USPTO is respectfully requested to deem the Postcard enclosed as Exhibit 2 as evidence of the response being received by the USPTO.

3. The USPTO is respectfully requested to withdraw the Notice of Abandonment dated January 7, 2008.

4. Further, the USPTO is respectfully requested to resume prosecution of the present application.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being transmitted electronically to the United States Patent and Trademark Office (USPTO) on the date shown below.

March 19, 2008
(Date of Transmission)

Stacey Dawson
(Name of Person Transmitting)

Stacey Dawson
(Signature)

3-19-08
(Date)

Respectfully submitted,

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile

```
Enclosures:     Statement as Setforth in 37 CFR 1.8(b)(3)
                Exhibit 1
                Exhibit 2
```

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Liqun Chen	)	Examiner: Simitoski, M.J.
		)	
Serial No.	10/613,750	)	Art Unit: 2134
		)	
Filed:	7/3/2003	)	Our Ref: B-5154 621086-5 300201957-3
For:	"Method and Apparatus for Generating a Cryptographic Key")	)	Date: March 19, 2008
		)	Re: *Statement as setforth in 37 CFR 1.8(b)(3)*
		)	
		)	

STATEMENT as setforth in 37 CFR 1.8(b)(3)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

I, Richard P. Berg, attorney of record for the above-referenced applicant, hereby declare that on August 15, 2007 I personally deposited with the United States Post Office a response to the Official Action dated May 15, 2007. I assert that the papers mailed contained the following:

1. a Response to Official Action
2. a Certificate of Mailing signed and dated August 15, 2007; and
3. a postcard.

Attached hereto is a copy of the response and postcard which were mailed on August 15, 2007.

Withdrawal of the holding of the abandonment issue is respectfully requested.

I hereby further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby certify that this correspondence is being transmitted electronically to the United States Patent and Trademark Office (USPTO) on the date shown below.

March 19, 2008
(Date of Transmission)

Stacey Dawson
(Name of Person Transmitting)

Stacey Dawson
(Signature)

3-19-08
(Date)

Respectfully submitted,

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile

EXHIBIT 1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Liqun Chen	)	Examiner:	Simitoski, M.J.
		)		
Serial No.	10/613,750	)	Art Unit:	2134
		)		
Filed:	7/3/2003	)	Our Ref:	B-5154 621086-5
		)		300201957-3
For:	"Method and Apparatus for Generating a Cryptographic Key"	)	Date:	August 15, 2007
		)	Re:	*Response*
		)		

RESPONSE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is filed in response to the Official Action dated May 15, 2007.

Specification amendments appear on page 2 of this response, a drawing amendment appears on page 3 thereof and claim amendments begin on page 4 thereof. Applicant's remarks, which are made without prejudice, begin on page 16 of this response.

Please amend the following paragraphs of the specification in the manner indicated:

[0067] is readily demonstrated. For example, starting with the encryption element *Enc*

$$\left[\left[\prod_{1\le i\le n} t(R_{TAi}P,\ rQ_{IDi})^{b_i} = \prod_{1\le i\le n} t(siP,\ rQ_{IDi})^{b_i}\right]\right]$$

$$\underline{\prod_{1\le i\le n} t(R_{TAi},\ rQ_{IDi})^{b_i} = \prod_{1\le i\le n} t(siP,\ rQ_{IDi})^{b_i}}$$

$$= \prod_{1\le i\le n} t(rP,\ siQ_{IDi})^{b_i}$$

$$= t\left(rP, \sum_{1\le i\le n} b_i s_i Q_{IDi}\right)$$

$$= t\left(U, \sum_{1\le i\le n} b_i s_i Q_{IDi}\right)$$

$$= t\left(U, \sum_{1\le i\le n} b_i s_i\right)$$

Please replace Figure 3 with the amended version of same enclosed herewith. The identity and TA elements of the decryption key (private - in the dashed line box) for the first embodiment used the term S_{IDi} whereas the description used the term S_i. See paragraph 0060. So in the amended figure, the term S_{IDi} is replaced with the term S_i in the first embodiment. Additionally, Ppubli (second embodiment, general form) has been changed to P_{publi} to be consistent with the description (see paragraph 0072).

Please amend the claims to read as indicated in the following list of claims:

Claims 1- 33. Cancelled.

34. [Currently amended] A method of generating an identifier-based asymmetric cryptographic key concerning a user with which multiple independent user identities are associated, each user identity being intended for use by a respective trusted authority; the method comprising using computer equipment to apply ~~wherein~~ a bilinear mapping function ~~is used~~ to process multiple data sets each comprising data related to ~~a respective association of trusted authority and~~ the user's identity with a respective one of the trusted authorities and data related to a secret held by that trusted authority, the secrets of the trusted authorities being unrelated to each other.

35. [Currently amended] A method according to claim 34, wherein the cryptographic key is an encryption key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on ~~a~~ the secret of the latter.

36. [Currently amended] A method according to claim 34, wherein the cryptographic key is a decryption key, each data set comprising an identity-based private key derived from said user identity and ~~a~~ the secret of the trusted authority.

37. [Currently amended] A method according to claim 34, wherein the cryptographic key is a signature key, each data set comprising an identity-based private key derived from said user identity and ~~a~~ the secret of the trusted authority.

38. [Currently amended] A method according to claim 34, wherein the cryptographic key is a verification key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on ~~a~~ the secret of the latter.

Claims 39 - 42. Cancelled

43. [Currently amended] A computer program product arranged, when installed in computing apparatus, to condition the apparatus for generating an identifier-based asymmetric cryptographic key concerning a user with which multiple independent user identities are associated, each user identity being intended for use by a respective trusted authority, the conditioned apparatus ~~by~~ using a bilinear mapping function to process multiple data sets each comprising data related to ~~a respective association of trusted authority and~~ the user's identity with a respective one of the trusted authorities and data related to a secret held by that trusted authority, the secrets of the trusted authorities being unrelated to each other; data from the multiple data sets being combined either before or after processing by the bilinear mapping function.

44. [Original] A method according to claim 35, wherein there are n data sets and the encryption key is generated as:

$$\prod_{1 \leq i \leq n} p\,(R_{TAi}, r\,Q_{IDi})$$

where:

$p()$ is said bilinear mapping function,

Q_{IDi} is the identity-based public key associated with the ith data set,

R_{TAi} is the public key element of the trusted authority associated with the ith data set, and

r is a random number.

45. [Original] A method according to claim 36, wherein there are n data sets and the decryption key is generated as:

$$p\,(U, \sum_{1 \leq i \leq n} S_i)$$

where:

$p()$ is said bilinear mapping function,

S_i is the identity-based private key associated with the ith data set, and

U is an element based on a random number and an element of a public key of the trusted authority associated with the ith data set.

46. [Original] A method according to claim 37, wherein there are n data sets and the signature key is generated as:

$$p\,(\Sigma_{(1 \leq i \leq n)} d_{IDi}, P)$$

where:

$p()$ is said bilinear mapping function,

d_{IDi} is the identity-based private key associated with the ith data set, and

P is a public key element of the trusted authority associated with the ith data set.

47. [Original] A method according to claim 38, wherein there are n data sets and the verification key is generated as:

$\Pi_{(1 \leq i \leq n)} p\,(Q_{IDi}, P_{pubi})$

where:

$p()$ is said bilinear mapping function,

Q_{IDi} is the identity-based public key associated with the ith data set, and

P_{pubi} is the public key element of the trusted authority associated with the ith data set.

48. [Currently Amended] A method according to claim 34, wherein:

the user identity and trusted authority of each data set are each associated with a respective point on an elliptic curve;

the point associated with the user identity is formed by a map-to-point hash function applied to the user identity, the combination of this point with a secret of the trusted authority forming an identity-based private key; and

the point associated with the trusted authority forms, together with a combination of this point with ~~a~~ the secret of the trusted authority, a public key of the trusted authority.

49. [Original] A method according to claim 34, wherein the bilinear mapping function pairing is one of a Tate pairing and a Weil pairing.

50. [New] A method according to claim 34, wherein data from the multiple data sets are combined before processing by the bilinear mapping function.

51. [New] A method according to claim 34, wherein data from the multiple data sets are combined after processing by the bilinear mapping function.

52. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key concerning a user with which multiple independent user identities are associated, each user identity being intended for use by a respective trusted authority, the computer apparatus using a bilinear mapping function to process multiple data sets each comprising data related to the user's identity with a respective one of the trusted authorities and data related to a secret held by that trusted authority, the secrets of the trusted authorities being unrelated to each other.

53. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein the cryptographic key is an encryption key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on the secret of the latter.

54. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein the cryptographic key is a decryption key, each data set comprising an identity-based private key derived from said user identity and the secret of the trusted authority.

55. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein the cryptographic key is a signature key, each data set comprising an identity-based private key derived from said user identity and the secret of the trusted authority.

56. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein the cryptographic key is a verification key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on the secret of the latter.

57. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 53, wherein there are n data sets and the encryption key is generated as:

$$\prod_{1 \le i \le n} p\,(R_{\mathrm{TA}i}, r\,Q_{\mathrm{ID}i})$$

where:

$p()$ is said bilinear mapping function,

$Q_{\mathrm{ID}i}$ is the identity-based public key associated with the ith data set,

$R_{\mathrm{TA}i}$ is the public key element of the trusted authority associated with the ith data set, and

r is a random number.

58. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 54, wherein there are n data sets and the decryption key is generated as:

$p\,(U, \sum_{1 \leq i \leq n} S_i)$

where:

$p()$ is said bilinear mapping function,

S_i is the identity-based private key associated with the ith data set, and

U is an element based on a random number and an element of a public key of the trusted authority associated with the ith data set.

59. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 55, wherein there are n data sets and the signature key is generated as:

$p\,(\Sigma_{(1 \leq i \leq n)} d_{\mathrm{IDi}}, P)$

where:

$p()$ is said bilinear mapping function,

$d_{\mathrm{ID}i}$ is the identity-based private key associated with the ith data set, and

P is a public key element of the trusted authority associated with the ith data set.

60. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 56, wherein there are n data sets and the verification key is generated as:

$$\Pi_{(1 \le i \le n)} p\,(Q_{\mathrm{ID}i}, P_{pubi})$$

where:

$p()$ is said bilinear mapping function,

$Q_{\mathrm{ID}i}$ is the identity-based public key associated with the i^{th} data set, and

$P_{\mathrm{pub}i}$ is the public key element of the trusted authority associated with the i^{th} data set.

61. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein:

the user identity and trusted authority of each data set are each associated with a respective point on an elliptic curve;

the point associated with the user identity is formed by a map-to-point hash function applied to the user identity, the combination of this point with a secret of the trusted authority forming an identity-based private key; and

the point associated with the trusted authority forms, together with a combination of this point with the secret of the trusted authority, a public key of the trusted authority.

62. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to

claim 52, wherein the bilinear mapping function pairing is one of a Tate pairing and a Weil pairing.

63. [New] The computer apparatus of claim 52 wherein data from the multiple data sets are combined before processing by the bilinear mapping function.

64. [New] The computer apparatus of claim 52 wherein data from the multiple data sets are combined after processing by the bilinear mapping function.

65. [New] A computer program product as for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the cryptographic key is an encryption key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on the secret of the latter.

66. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the cryptographic key is a decryption key, each data set comprising an identity-based private key derived from said user identity and the secret of the trusted authority.

67. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the cryptographic key is a signature key, each data set comprising an identity-based private key

derived from said user identity and the secret of the trusted authority.

68. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the cryptographic key is a verification key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on the secret of the latter.

69. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 65, wherein there are n data sets and the encryption key is generated as:

$$\prod_{1 \le i \le n} p\,(R_{TAi}, r\, Q_{IDi})$$

where:

$p()$ is said bilinear mapping function,

Q_{IDi} is the identity-based public key associated with the i^th^ data set,

R_{TAi} is the public key element of the trusted authority associated with the i^th^ data set, and

r is a random number.

70. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 66, wherein there are n data sets and the decryption key is generated as:

$$p\,(U, \textstyle\sum_{1 \le i \le n} S_i)$$

where:

$p()$ is said bilinear mapping function,

S_i is the identity-based private key associated with the ith data set, and

U is an element based on a random number and an element of a public key of the trusted authority associated with the ith data set.

71. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 67, wherein there are n data sets and the signature key is generated as:

$p\,(\Sigma_{(1 \leq i \leq n)}\, d_{\mathrm{IDi}}, P)$

where:

$p()$ is said bilinear mapping function,

$d_{\mathrm{ID}i}$ is the identity-based private key associated with the ith data set, and

P is a public key element of the trusted authority associated with the ith data set.

72. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 68, wherein there are n data sets and the verification key is generated as:

$\Pi_{(1 \leq i \leq n)}\, p\,(Q_{\mathrm{IDi}}, P_{pubi})$

where:

$p()$ is said bilinear mapping function,

$Q_{\mathrm{ID}i}$ is the identity-based public key associated with the ith data set, and

$P_{\mathrm{pub}i}$ is the public key element of the trusted authority associated with the ith data set.

73. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein:

the user identity and trusted authority of each data set are each associated with a respective point on an elliptic curve;

the point associated with the user identity is formed by a map-to-point hash function applied to the user identity, the combination of this point with a secret of the trusted authority forming an identity-based private key; and

the point associated with the trusted authority forms, together with a combination of this point with the secret of the trusted authority, a public key of the trusted authority.

74. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the bilinear mapping function pairing is one of a Tate pairing and a Weil pairing.

75. [New] The computer program product of claim 43 wherein data from the multiple data sets are combined before processing by the bilinear mapping function.

76. [New] The computer program product of claim 43 wherein data from the multiple data sets are combined after processing by the bilinear mapping function.

REMARKS/ARGUMENTS

Claims 1-33 and 39-42 have been cancelled without prejudice.

Claim 34

Claim 34 was rejected as being anticipated by US Patent Pub 2003/0179885 to Gentry. Claim 34 has been amended to more clearly differentiate it from Gentry.

The main changes made to claim 34 are:

1. The key generated by the method is now specified as being:

"an identifier-based asymmetric cryptographic key"

All the described embodiments generate such keys as can be readily appreciated by reference to Figure 3 and the section headed "Review" on page 16 of the application as filed.

2. Associated with the user are:

"multiple independent identities ..., each identity being intended for use by a respective trusted authority"

Again, all the described embodiments exhibit this feature and the paragraph spanning pages 9 and 10 of the application as filed describes this feature.

3. The secrets of the trusted authorities are specified as:

"the secrets of the trusted authorities being unrelated to each other"

That the secrets of the trusted authorities are unrelated is clear from the description - see, for example, page 9 line 16 which discloses that the trusted authorities "have their own respective random secrets", it being understood that the randomness of the secrets ensures that they are unrelated. This quoted feature was introduce to further distinguish claim 34 from the Boneh and Franklin paper.

The corresponding claim in the corresponding EP claim ends with the phrase:

"data from the multiple data sets being combined either before or after processing by the bilinear mapping function"

Since this sort of limitation often attracts an objection in the US, a respective dependent claim to each possibility has been added as new claims 50 and 51. Support is easy to spot from the column headed 'General Form' in Figure 3, for examples of either possibility.

The second of the above new features of claim 34 provides the clearest point of difference from the Gentry reference (US 2003/0179885). In Gentry, as is described in paragraph 0085 thereof, the recipient z is associated with the ID-tuple:

$$(ID_{z1},\ldots.., ID_{z(n+1)})$$

This ID-tuple is made up of identity information $ID_{z(n+1)}$ associated with the recipient z and identity information ID_{zi} associated with each of the recipient's n ancestral lower-level PKGs in the hierarchy. In other words, each PKG and the recipient has an identity label that is not necessarily unique in itself but when collected in order from the root to the recipient (or, indeed, in reverse from the recipient to the root) they make up a unique identity for the recipient z. This is succinctly put at the top of page 551 of the Gentry paper:

> "**ID-Tuple:** A user has a position in the hierarchy, defined by its tuple of IDs: $(ID_1,\ldots.., ID_t)$. The user's ancestors in the hierarchy tree are the root PKG and the users/lower-level PKGs whose ID-tuples are $\{(ID_1,\ldots.., ID_i) : 1 \leq i \leq t\}$."

(The IDs referred to in the first line of this definition are clearly not all IDs of the user since the second sentence makes it clear that an ancestor user / lower-level PKG has an ID-tuple made up of a subset of these IDs).

Of course, ID-tuples like this are very common, two examples being domain names and street addresses (though both are usually written in reverse order).

The important point is that the recipient has only one piece of identity information associated with it ($ID_{z(n+1)}$) and only one unique identity – the ID-tuple. The identity information ID_{zi} associated with each ancestor PKG of the recipient is not specific to the recipient – any party directly or indirectly dependent from a given PKG will have the identity information of that PKG in the ID-tuple of that party. Thus Gentry does not disclose or suggest the user having:

> "multiple independent identities …, each identity being intended for use by a respective trusted authority"

as is recited in amended claim 34.

At the top of page 6 of the Action, the examiner asserts that Gentry discloses the use of different user identities by referring to the elements U_0 to U_{n+1}. However, U_i=rP_{zi} and the elements P_{zi} for $1 \leq i \leq n$ are public elements of the recipients ancestral PKG (see [0086]) and not of the recipient; only U_{n+1} (= rPz(n+1)) uses the identity information of the recipient – in particular:

$P_{z(n+1)} = H_1(ID_{z1},\ldots..,\ ID_{z(n+1)})$

where :

$ID_{z(n+1)}$ is the identity information of the recipient, and

$(ID_{z1},\ldots.., ID_{z(n+1)})$ is the ID-tuple of the recipient (the only true identifier of the recipient).

Claim 34 is also being amended to recite "using computer equipment to apply ..." to make it clear that the claim is directed to statutory subject matter.

Claim 43

Claim 43 has amended in a similar manner to the amendments made to claim 34 therefor it should be in condition for allowance.

New dependent claims 65-76 have been added which depend from claim 43 and which are patterned after the claims dependent upon claim 34.

Claim 52

Claim 52 is a new apparatus claims and its general similarity with claim 34 should be apparent and it is believed that it too distinguishes itself from the prior art.

New dependent claims 53-64 have also been added which depend from claim 52 and which are patterned after the claims dependent upon claim 34.

Figure 3

A replacement figure 3 is enclosed which corrects, as described above, minor editorial errors noted in the original version thereof.

Specification Amendment

A error was noted in the first equation of paragraph 0067 where are extra "P" occurred in the original. This amendment brings the equation into line with the disclosure at paragraph 0066.

IDS

An IDS is enclosed herewith. Enclosed therewith is an official action dated March 18, 2204, in which the European Examiner cited Boneh (which was previously cited in an IDS filed in this application.) Differentiating arguments can be found in the EP response dated June 28, 2004, a copy of which also accompanies the IDS.

The Shamir secret sharing paper listed in the IDS is cited the response dated June 28, 2004 filed in the corresponding EP application.

Two further official actions issued in respect of the corresponding EP application, but no additional prior art was cited against the claims, but clarity issues were raised. The Examiner is invited to review the prosecution history of the corresponding EP application at http://www.epoline.org/portal/public/registerplus by providing the application number of the EP application (03254262).

Withdrawal of the rejections and allowance of the claims are respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2125. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2125.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

August 15, 2007
(Date of Transmission)

Richard Berg
(Name of Person Transmitting)

(Signature)

August 15, 2007
(Date)

Respectfully submitted,

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile

Embodiment	Key Type	Identity Element	TA Element	Session Element	General Form
First	Encryption “Enc”	Q_{IDi} Public	R_{TAi} Public	r Private	$\prod t(R_{TAi}, rQ_{IDi})$
	Decryption “Dec”	S_i Private Q_{IDi} in S_i	s_i in S_i	U Public	$t(U, \sum b_i S_i)$
Second	Encryption “gID”	Q_{IDi} Public	P_{pubi} Public	σ Private	$\Pi\hat{e}(Q_{IDi}, P_{pubi})$
	Decryption “x”	d_{IDi} Private Q_{IDi} in d_{IDi}	s_i in d_{IDi}	U Public	$\hat{e}(\Sigma\, d_{IDi}, U)$
Third	Signature (compound)	d_{IDi} Private	P_{pubi} Public	z Private	$h\,\Sigma\, d_{IDi} + z\,\Sigma P_{pubi}$
	Verification (compound)	Q_{IDi} Public	P_{pubi}, U Public	U Public	$\Pi\hat{e}(P_{pubi}, hQ_{IDi} + U)$
Fourth	Signature “e”	d_{IDi} Private Q_{IDi} in d_{IDi}	s_i in d_{IDi}	k Private	$\hat{e}(\Sigma\, d_{IDi}, P)$
	Verification ’’’e’’’	Q_{IDi} Public	P_{pubi} Public	h, S Public	$\Pi\hat{e}(Q_{IDi}, P_{pubi})$

Figure 3

EXHIBIT 2

TO: RPB -

FROM: **COMMISSIONER OF PATENTS AND TRADEMARKS**

OUR REF: 621086

DATE MAILED 15 Aug 2007

THE PATENT AND TRADEMARK OFFICE MAIL ROOM STAMP HEREON ACKNOWLEDGES

RECEIPT OF: Response (21 pages) with certificate of mailing; Fig 3; IDS (3p) with cert. of mailing and copy of each cited ref.

IN CONNECTION WITH: LIQUIN CHEN

SERIAL NUMBER 10/613750

STAMP

M/RPS

LADAS & PARRY
5670 Wilshire Blvd., Suite 2100
Los Angeles, CA 90036